Document

Select the documents you wish to save or order by clicking the box next to the document, or click the link above the document to order directly.

☑ **document 4 of 5** Order Document

INSPEC - 1969 to date (INZZ)

Accession number & update
7213703, B2002-04-6135C-167, C2002-04-6130S-060; 20020325.

Title
Invertible authentication.

Author(s)
Fridrich-J; Goljan-M; Rui-Du.

Author affiliation
Center for Intelligent Syst, State Univ of New York, Binghamton, NY, USA.

Source
Security and Watermarking of Multimedia Contents III, San Jose, CA, USA, 22-25 Jan. 2001.
Sponsors: SPIE.
In: Proceedings-of-the-SPIE-The-International-Society-for-Optical-Engineering (USA), vol.4314, p.197-208, 2001.

CODEN
PSISDG.

ISSN
ISSN: 0277-786X, CCCC: 0277-786X/01/ ($15.00).

Availability
SICI: 0277-786X(2001)4314L.197:IA; 1-7.

Publication year
2001.

Language
EN.

Publication type
CPP Conference Paper, J Journal Paper.

Treatment codes
P Practical.

Abstract
We present two new methods for **authentication** of digital images using **invertible** watermarking: one is based on robust spatial additive watermarks combined with modulo addition and the second one is based on lossless compression and encryption of bit-planes. Both techniques provide cryptographic strength in verifying the image integrity in the sense that the probability of making a modification to the image that will not be detected can be directly related to a secure cryptographic element, such as a hash function. The second technique can be generalized to data types other than bitmap images. As an

example, a lossless **authentication** method for JPEG files is presented and some results discussed. We also explain that **invertible authentication** can only be achieved at the expense of not being able to authenticate every possible image. However, it is argued that all images that occur in practice can be authenticated. The techniques provide new information assurance tools for integrity protection of sensitive imagery, such as medical images or images viewed under nonstandard conditions when usual criteria for visibility do not apply. (17 refs).

Descriptors

copy-protection; cryptography; data-compression; data-integrity; image-coding; message-authentication.

Keywords

invertible authentication; digital image **authentication; invertible** watermarking; robust spatial additive watermarks; modulo addition; lossless compression; bit plane encryption; cryptographic strength; image integrity; probability; secure cryptographic element; hash function; data types; bitmap images; lossless **authentication** method; JPEG files; information assurance tools; integrity protection; sensitive imagery; digital watermarking.

Classification codes

```
B6135C    (Image and video coding).
B6120B    (Codes).
B6120D    (Cryptography).
C6130S    (Data security).
C1260S    (Signal processing theory).
C5260B    (Computer vision and image processing techniques).
```